MATH 845: HOMEWORK 3, DUE MAR 11.

5. Let E be the elliptic curve $y^2 + y = x^3 - x$, with group law identity $(0, 1, 0)$. Let K_m denote the extension of $\mathbf{Q}$ generated by the coordinates of all the points P in $E[m] := \{P \in E(\overline{\mathbf{Q}}) \mid mP = \text{identity}\}$.

(a) Show that K_m is a Galois extension of $\mathbf{Q}$ and that the Galois group of this extension is a subgroup of $GL_2(\mathbf{Z}/m)$.

(b) What is $[K_2 : \mathbf{Q}]$?

(c) What is $[K_3 : \mathbf{Q}]$? [Suggestion: note that $GL_2(\mathbf{Z}/3)/\text{scalars} = PGL_2(\mathbf{Z}/3) \cong S_4$. Which subgroups of $GL_2(\mathbf{Z}/3)$ have S_4 as a quotient?]

6. (a) Let $g = x^3y + y^3z + z^3x \in \mathbf{F}_q[x, y, z]$. Let V be the projective curve given by $g = 0$. Find the zeta function of V for $q = 2$ and $q = 3$.

(b) Let $f = x^{q+1} - y^q - y \in \mathbf{F}_{q^2}[x, y]$ (q a prime power). Let C be the projective curve over $\mathbf{F}_{q^2}$ defined by f. Show that $t^q + t + 1, t^{q+1} + 1$ have roots $\alpha, \beta \in \mathbf{F}_{q^2}$ respectively. Show that if $x^{q+1} + y^{q+1} + 1 = 0$, then $\beta x \neq y$ and setting $u = \beta/(y - \beta x), v = ux - \alpha$, then $f(u, v) = 0$. How large is $\#C(\mathbf{F}_{q^2})$?